

### REMARKS

Applicant gratefully acknowledges the courtesy of the Examiner in granting an interview to Applicant's representative Sanford T. Colb, registration number 26,856, on 19 October 2004. In the interview, the difference between the prior art of record and the present invention in general, and claims 78 and 84 in particular, was discussed. More particularly, the lack of transfer of the disk key in the absence of prior player authentication (as recited in claim 83 before the present amendment) was discussed. Furthermore, claim 84 was discussed regarding the feature that the disk key is encrypted with the player key. The examiner suggested filing the present after final response to allow the examiner to fully consider the points raised in the interview. DVD CSS was mentioned by the Examiner as an area which the Examiner might wish to search further in regard to claims 78 and 84.

Applicant has carefully studied the outstanding Official Action. The present amendment is intended to be fully responsive to all points of rejection and is believed to place the application in condition for allowance. Favorable reconsideration and allowance of the present application are hereby respectfully requested.

Claims 52 - 78, 80 - 86 and 88 - 95 stand as rejected in the present application.

Claims 52 - 57, 59 - 63, 66, 68 - 69, 71 - 75, 78, 80 - 81, 83 - 84, and 89 - 92 stand rejected under 35 USC 103(a) as being unpatentable over US Patent 5,881,152 to Moos, and further in view of IBM TDB NN85122861 of Anon and US Patent 5,445,532 to Evans.

Moos describes a process and device for combining non-intelligent generic information storage devices with intelligent storage devices and linking their information. The process compresses the stored data from a generic storage device and counts a signature count of the stored data. An ID is then provided to the stored data from a permanently assigned intelligent programmable memory chip. At least part of the compressed data is encrypted using an asymmetric key and transferred to a memory area of the permanently assigned intelligent programmable memory chip.

Anon describes a magnetic recording disk file with a silicon substrate disk containing both integrated electronic circuits and magnetic media. Flexible wires or conductors connect the integrated circuits on the sides of the disks to a rotor.

Evans describes a novel form of socket for integrated circuits to be mounted on printed circuit boards. The socket uses a novel contact which is fabricated out of a bimetallic strip with a shape which makes the end of the strip move laterally as temperature changes. The end of the strip forms a barb which digs into an integrated circuit lead at normal temperatures and holds it firmly in the contact, preventing loosening and open circuits from vibration. By cooling the contact containing the bimetallic strip the barb end can be made to release so that the integrated circuit lead can be removed from the socket without damage either to the lead or to the socket components.

Applicants have carefully reviewed the references and find that:

the references do not show transmitting a key;

the references do not show transmitting a key which protects content; and

the references do not require first showing authenticity before sending a key.

Therefore, the limitations of claim 83 have been written into claim 78 in order to distinctly clarify the differences between the present invention as claimed in claim 78, as pointed out above, and the references cited.

Amended claim 78 is therefore deemed allowable.

Claims 80 - 81 and 84 depend from amended claim 78 and recite additional patentable subject matter.

Particularly in regard to claim 84, all three of the properties mentioned above as distinguishing the present invention over the cited references, are found. Claim 84 recites: "The method according to claim 78 and wherein said disk security chip, after assuring that said DVD player is authentic, sends said DVD player said disk key encrypted with said player key."

The property, lacking in the references cited, of transmitting a key, is, by contrast, found in claim 84: "said disk security chip, ... sends said DVD player said disk key".

The property, lacking in the references cited, of transmitting a key which protects content, is, by contrast, found in claim 84: "...sends said DVD player said disk key".

The property, lacking in the references cited, of requiring a showing of authenticity before sending a key, is, by contrast, found in claim 84: "...after assuring that said DVD player is authentic, sends said DVD player said disk key".

Claims 80 - 81 and 84 are therefore deemed allowable.

Claims 52 - 57, 59 - 63, 66, 68 - 69, 71 - 75, 83, and 89 - 92 have been cancelled without prejudice. Applicants reserve the right to pursue claims 52 - 57, 59 - 63, 66, 68 - 69, 71 - 75, 83, and 89 - 92 in a continuation application.

Claims 58 and 70 stand rejected under 35 USC 103(a) as being unpatentable over Moos/Anon and further in view of Olukotun et al., The Case for a Single-chip Multiprocessor (1996). Claims 58 and 70 also stand rejected under 35 USC 103(a) as being unpatentable over Moos/Anon and further in view of Anderson et al., Tamper Resistance - a Cautionary Note (1996).

Olukotun et al. describe how, using advanced technologies, it is possible to implement a single-chip multiprocessor in the same area as a wide issue superscalar processor. For applications with large parallelism at both the fine and coarse grained levels, the multiprocessor architecture outperforms the superscalar architecture by a significant margin. Single-chip multiprocessor architectures have the advantage in that they offer localized implementation of a high-clock rate processor for inherently sequential applications and low latency interprocessor communication for parallel applications.

Anderson et al. describe a number of different types of attacks on systems that rely on the tamper resistance of smart cards and other security processors. Anderson et al. concludes that trusting tamper resistance is problematic. Smart cards are routinely broken.

Claims 58 and 70 have been cancelled without prejudice. Applicants reserve the right to pursue claims 58 and 70 in a continuation application.

Claims 64 - 65, 76 - 77, 85 - 86 and 88 stand rejected under 35 USC 103(a) as being unpatentable over Moos/Anon in view of US Patent 5,988,500 to Litman.

Litman describes a system and method of inserting magnetic elements into items in order to provide readable magnetic patterns which provide reproducible or unique signals to identify or authenticate items.

Claims 85 - 86 depend, either directly or indirectly from claim 78 and recite additional patentable subject matter.

Claims 85 - 86 are therefore deemed allowable with reference to the above discussion of the allowability of claim 78.

Claims 64 - 65, 76 - 77, and 88 have been cancelled without prejudice. Applicants reserve the right to pursue claims 64 - 65, 76 - 77, and 88 in a continuation application.

Claims 67, 82 and 93 stand rejected under 35 USC 103(a) as being unpatentable over Moos/Anon/Litman, and further in view of Menezes et al., Handbook of Applied Cryptography (1997), pages 406 - 410.

Menezes et al., on pages 406 - 410 describe zero knowledge identification protocols.

Claim 82 depends from claim 78 and recites additional patentable subject matter.

Claim 82 is therefore deemed allowable with reference to the above discussion of the allowability of claim 78.

Claims 67 and 93 have been cancelled without prejudice. Applicants reserve the right to pursue claims 67 and 93 in a continuation application.

Claims 93 - 95 stand rejected under 35 USC 103(a) as being unpatentable over Moos/Anon and further in view of Clark et al., A Survey of Authentication Protocol Literature (1997), pages 44 - 45.

Clark et al. describe symmetric key protocols without a trusted third party. Particularly, ISO symmetric key one-, two- and three-pass unilateral authentication protocols, are described on the cited pages.

Claims 93 - 95 have been cancelled without prejudice. Applicants reserve the right to pursue claims 93 - 95 in a continuation application.

In view of the foregoing remarks, it is respectfully submitted that the present application is now in condition for allowance. Favorable reconsideration and allowance of the present application are respectfully requested.

Respectfully submitted,

A handwritten signature in black ink, appearing to read 'Julian H. Cohen', is written over a horizontal line.

JULIAN H. COHEN  
LADAS & PARRY LLP  
26 WEST 61ST STREET  
NEW YORK, N.Y. 10023  
REG.NO.20302(212)708-1887